

SpiderFoot OSINT Tool - Complete Project Guide

Table of Contents

1. Introduction
2. What is SpiderFoot?
3. Key Features
4. System Requirements
5. Installation Guide
6. Configuration
7. Usage Guide
8. Command Reference
9. Practical Use Cases
10. Advantages and Disadvantages
11. Best Practices
12. Legal and Ethical Considerations
13. Resources

Introduction

This comprehensive guide provides everything you need to understand, install, configure, and effectively use SpiderFoot for Open Source Intelligence (OSINT) gathering. Whether you're a security professional, penetration tester, researcher, or cybersecurity enthusiast, this guide will walk you through every aspect of SpiderFoot.

What is SpiderFoot?

SpiderFoot is an open-source intelligence (OSINT) automation tool that integrates with multiple data sources to gather information about a target. It automates the process of collecting intelligence from over 200 public data sources including WHOIS records, DNS records, search engines, social media platforms, threat intelligence feeds, and more.

Definition

SpiderFoot is a reconnaissance tool designed to automate the OSINT gathering process by:

- Querying multiple data sources simultaneously
- Correlating discovered data to find relationships
- Presenting findings in an organized, actionable format
- Identifying potential security risks and exposure points

Purpose and Importance

Why SpiderFoot Matters:

1. **Comprehensive Reconnaissance:** Provides a 360-degree view of your digital footprint or target
2. **Time Efficiency:** Automates hours of manual OSINT work into minutes
3. **Threat Intelligence:** Identifies potential vulnerabilities and security exposures
4. **Attack Surface Mapping:** Discovers all internet-facing assets associated with a target
5. **Data Correlation:** Connects disparate pieces of information to reveal hidden relationships

System Requirements

Minimum Requirements

- **Operating System:** Linux, Windows, macOS
- **Python Version:** Python 3.7 or higher
- **RAM:** 2GB minimum (4GB recommended)
- **Disk Space:** 500MB for installation
- **Network:** Stable internet connection

Recommended Environment

- **OS:** Kali Linux, Ubuntu 20.04+, or Debian-based distributions
- **RAM:** 8GB
- **Processor:** Multi-core CPU
- **Network:** High-speed broadband connection

Installation Guide

Method 1: Installation on Linux (Ubuntu/Debian)

Step 1pi: Update System Packages

bash

```
sudo apt update && sudo apt upgrade -y
```

Step 2: Install Required Dependencies

bash

```
sudo apt install python3 python3-pip git -y
```

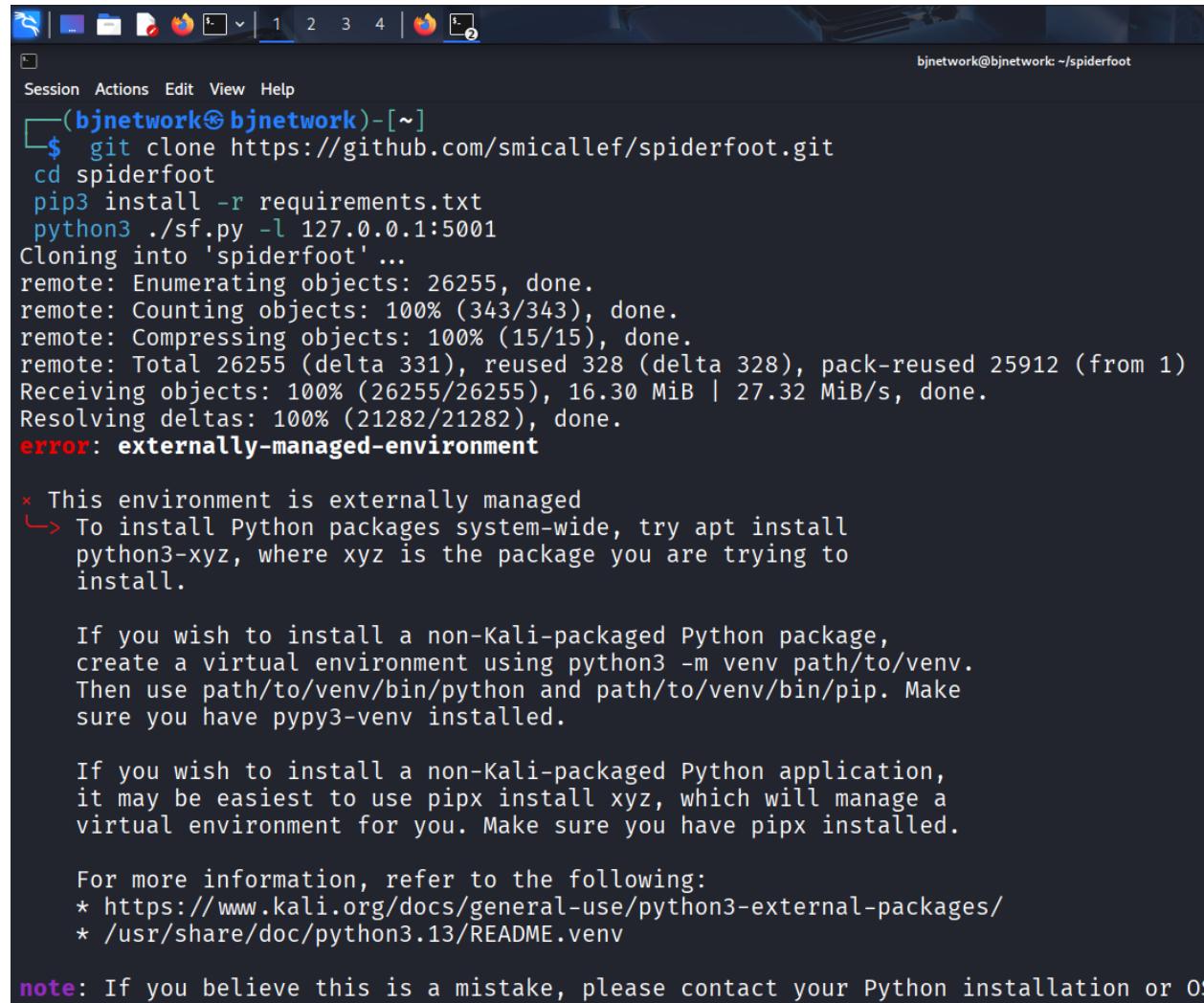
```
(bjnetwork㉿bjnetwork)-[~/spiderfoot]
$ sudo apt install python3 python3-pip git -y
python3 is already the newest version (3.13.7-1+b1).
python3-pip is already the newest version (25.3+dfsg-1).
python3-pip set to manually installed.
git is already the newest version (1:2.51.0-1).
git set to manually installed.
```

Step 3: Clone SpiderFoot Repository

```
cd ~
```

```
git clone https://github.com/smicallef/spiderfoot.git
```

```
cd spiderfoot
```



The screenshot shows a terminal window with a dark background. At the top, there's a header bar with icons for file, edit, and search, followed by tabs labeled 1, 2, 3, 4, and a Firefox icon. The title bar on the right says "bjnetwork@bjnetwork: ~/spiderfoot". The main area of the terminal shows the following command-line session:

```
(bjnetwork㉿bjnetwork)-[~]
$ git clone https://github.com/smicallef/spiderfoot.git
cd spiderfoot
pip3 install -r requirements.txt
python3 ./sf.py -l 127.0.0.1:5001
Cloning into 'spiderfoot'...
remote: Enumerating objects: 26255, done.
remote: Counting objects: 100% (343/343), done.
remote: Compressing objects: 100% (15/15), done.
remote: Total 26255 (delta 331), reused 328 (delta 328), pack-reused 25912 (from 1)
Receiving objects: 100% (26255/26255), 16.30 MiB | 27.32 MiB/s, done.
Resolving deltas: 100% (21282/21282), done.
error: externally-managed-environment

× This environment is externally managed
↳ To install Python packages system-wide, try apt install
  python3-xyz, where xyz is the package you are trying to
  install.

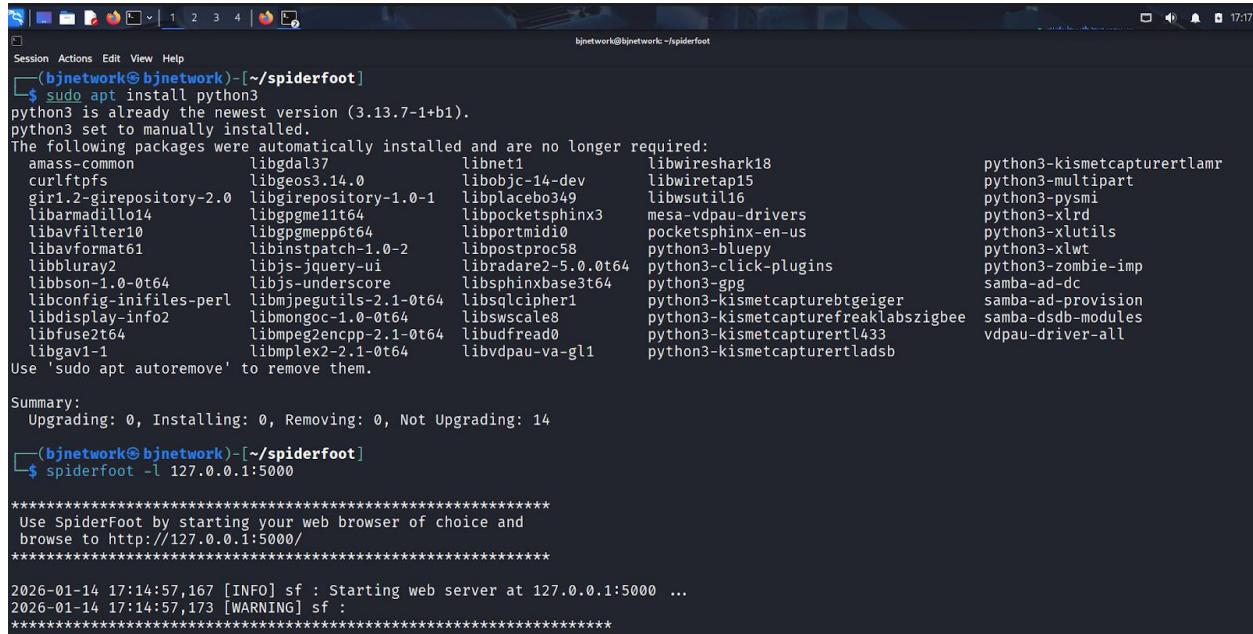
If you wish to install a non-Kali-packaged Python package,
create a virtual environment using python3 -m venv path/to/venv.
Then use path/to/venv/bin/python and path/to/venv/bin/pip. Make
sure you have pypy3-venv installed.

If you wish to install a non-Kali-packaged Python application,
it may be easiest to use pipx install xyz, which will manage a
virtual environment for you. Make sure you have pipx installed.

For more information, refer to the following:
* https://www.kali.org/docs/general-use/python3-external-packages/
* /usr/share/doc/python3.13/README.venv

note: If you believe this is a mistake, please contact your Python installation or OS
```

Step 4: Install Python Requirements



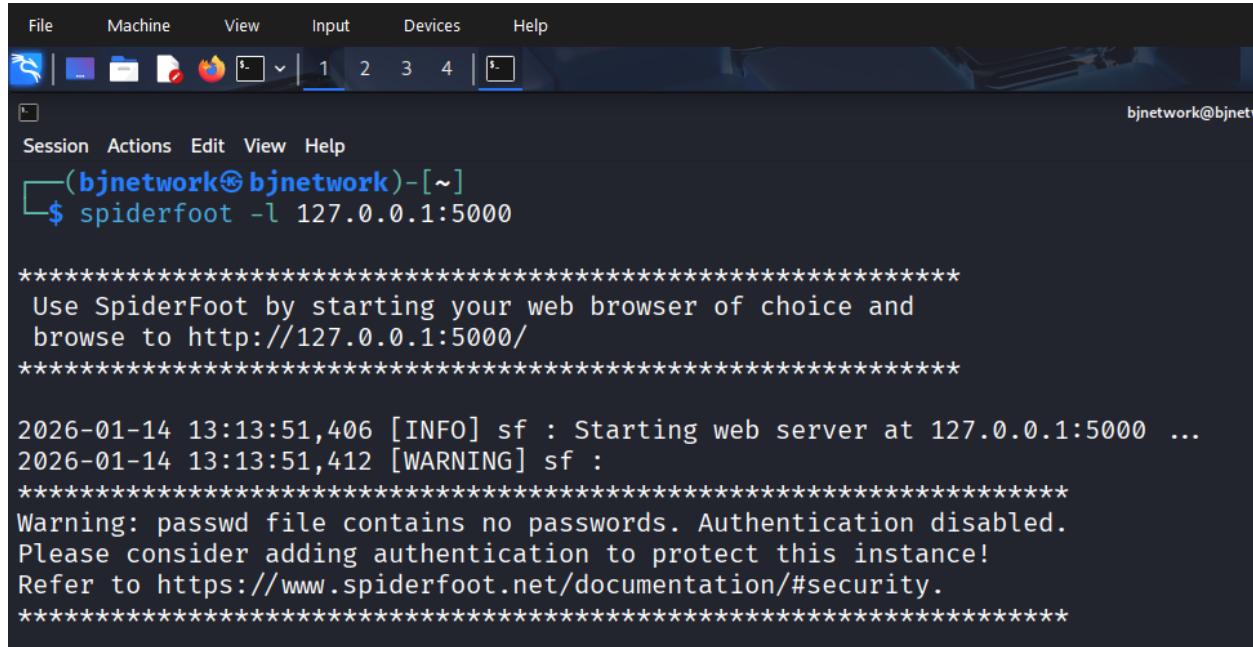
```
Session Actions Edit View Help
(bjnetwork@bjnetwork)-[~/spiderfoot]
$ sudo apt install python3
python3 is already the newest version (3.13.7-1+b1).
python3 set to manually installed.
The following packages were automatically installed and are no longer required:
  amass-common      libgdal37          libneti           libwireshark18
  curlftpfs        libgeos3.14.0       libobjc-14-dev    libwiretap15
  gir1.2-girepository-2.0 libgirepository-1.0-1 libplacebo349   libwsutil16
  libarmadillo4     libggme1t64        libpocketsphinx3 mesa-vdpau-drivers
  libavfilter10     libggmep6t64       libportmidi0    pocketsphinx-en-us
  libavformat61     libbinpatch-1.0-2  libpostproc58  python3-bluepy
  libbluray2        libjs-jquery-ui    libradare2-5.0.0t64 python3-click-plugins
  libbsone-1.0-0t64 libjs-underscore  libsshbase3t64  python3-gpg
  libconfig-inifiles-perl libjpeguilts-2.1-0t64 libsqlcipher1  python3-kismetcapturebtgeiger
  libdisplay-info2  libmongoc-1.0-0t64  libwscale8    python3-kismetcapturefreaklabszigbee
  libfuse2t64       libmpeg2encpp-2.1-0t64 libudfread0   python3-kismetcapturetl433
  libgav1-1         libmplex2-2.1-0t64  libvdpau-va-gli  python3-kismetcapturetladsb
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 14

(bjnetwork@bjnetwork)-[~/spiderfoot]
$ spiderfoot -l 127.0.0.1:5000
*****
Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:5000/
*****
2026-01-14 17:14:57,167 [INFO] sf : Starting web server at 127.0.0.1:5000 ...
2026-01-14 17:14:57,173 [WARNING] sf :
*****
```

Step 1: Start SpiderFoot

spiderfoot -l 127.0.0.1:5000

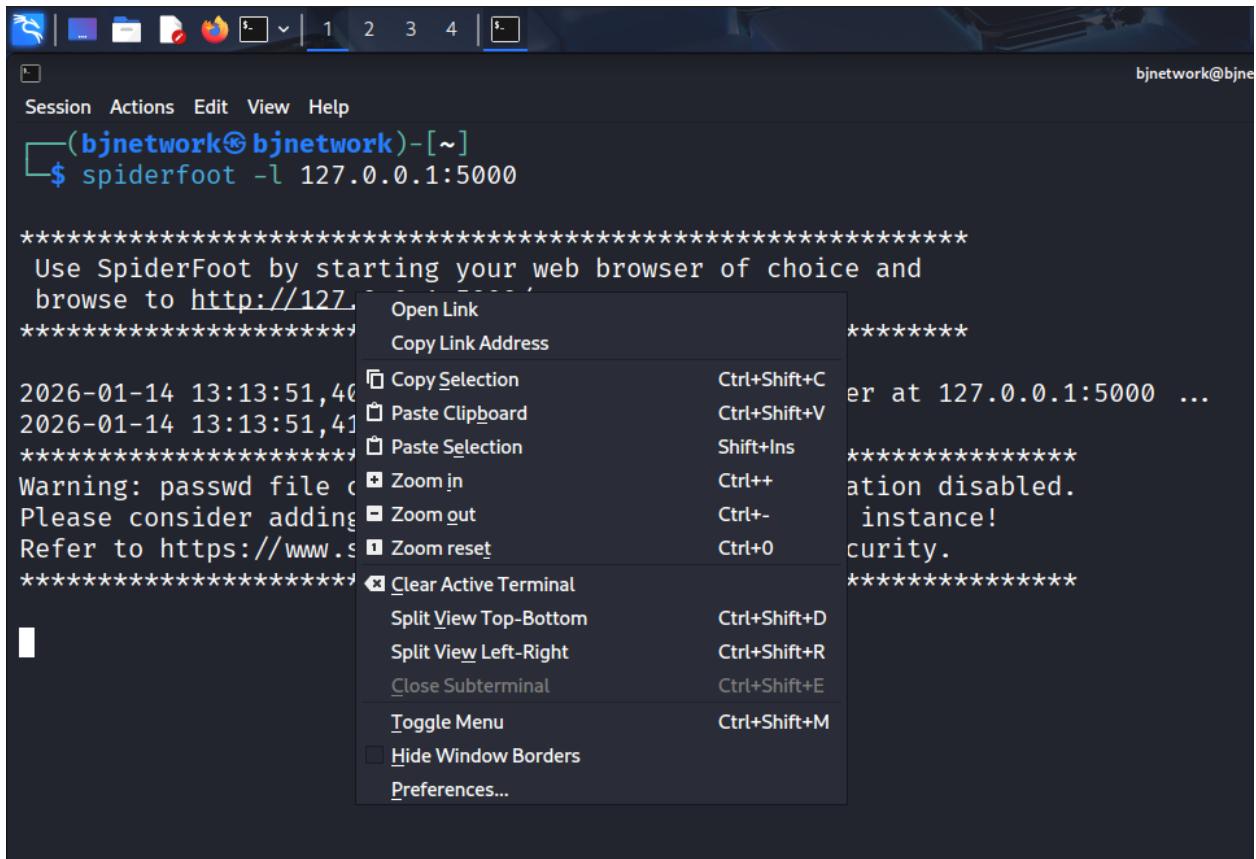


```
File Machine View Input Devices Help
Session Actions Edit View Help
(bjnetwork@bjnetwork)-[~]
$ spiderfoot -l 127.0.0.1:5000
*****
Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:5000/
*****
2026-01-14 13:13:51,406 [INFO] sf : Starting web server at 127.0.0.1:5000 ...
2026-01-14 13:13:51,412 [WARNING] sf :
*****
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
*****
```

Step 6: Access Web Interface

Open your browser and navigate to:

<http://127.0.0.1:5001>



The screenshot shows a terminal window with the following content:

```
(bjnetwork@bjnetwork)-[~]
$ spiderfoot -l 127.0.0.1:5000

*****
Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:5000 ...
*****
2026-01-14 13:13:51,40
2026-01-14 13:13:51,41
*****
Warning: passwd file could not be found.
Please consider adding it to the configuration.
Refer to https://www.spiderfoot.net/doc/config.html
*****
```

A context menu is open over the line "Use SpiderFoot by starting your web browser of choice and". The menu items are:

- Copy Link
- Copy Link Address
- Copy Selection (Ctrl+Shift+C)
- Paste Clipboard (Ctrl+Shift+V)
- Paste Selection (Shift+Ins)
- Zoom in (Ctrl++)
- Zoom out (Ctrl+-)
- Zoom reset (Ctrl+0)
- Clear Active Terminal
- Split View Top-Bottom (Ctrl+Shift+D)
- Split View Left-Right (Ctrl+Shift+R)
- Close Subterminal (Ctrl+Shift+E)
- Toggle Menu (Ctrl+Shift+M)
- Hide Window Borders
- Preferences...

Method 2: Docker Installation

Step 1: Install Docker

Follow instructions at docker.com

Step 2: Pull SpiderFoot Docker Image

bash

```
docker pull spiderfoot/spiderfoot
```

Step 3: Run SpiderFoot Container

bash

```
docker run -p 5001:5001 spiderfoot/spiderfoot
```

Step 4: Access Interface

Navigate to <http://localhost:5001>

Configuration

Initial Setup

Step 1: Access Settings

Once SpiderFoot is running, click on **Settings** in the web interface.

Global Settings	
Option	Value
Enable debugging?	False
Override the default resolver with another DNS server. For example, 8.8.8.8 is Google's open DNS server.	
Number of seconds before giving up on a HTTP request.	5
List of usernames that if found as usernames or as part of e-mail addresses, should be treated differently to non-generics.	abuse.admin,billing,compliance,devnull,dns,ftp,hostmaster,inoc,ispfeedback,
List of Internet TLDs.	https://publicsuffix.org/list/effective_tld_names.dat
Hours to cache the Internet TLD list. This can safely be quite a long time given that the list doesn't change too often.	72
Max number of modules to run concurrently	3
SOCKS Server Type. Can be '4', '5', 'HTTP' or	

Step 2: Configure API Keys (Optional but Recommended)

SpiderFoot works better with API keys for various services:

- **Shodan API:** For device and service discovery
- **VirusTotal API:** For malware and threat intelligence
- **HaveIBeenPwned API:** For breach data
- **AlienVault OTX API:** For threat intelligence
- **Censys API:** For internet-wide scanning data

How to add API keys:

1. Navigate to Settings → API Keys
2. Enter your API key for each service
3. Click Save

Step 3: Module Configuration

Enable or disable specific modules based on your needs:

1. Go to Settings → Modules
2. Check/uncheck modules you want to use
3. Save configuration

Usage Guide

Creating Your First Scan

Step 1: Start a New Scan

1. Click on **New Scan** from the main interface
2. Enter scan name (e.g., "Target Domain Reconnaissance")

The screenshot shows the SpiderFoot v4.0.0 web interface. At the top, there's a navigation bar with tabs like 'about:sessionrestore' and 'SpiderFoot v4.0.0'. Below the navigation bar, the URL is http://127.0.0.1:5000/newsScan. The main content area is titled 'New Scan'. It has two input fields: 'Scan Name' (containing 'The name of this scan.') and 'Scan Target' (containing 'The target of your scan.'). To the right of these fields is a help box with examples for various target types: Domain Name, IPv4 Address, IPv6 Address, Hostname/Sub-domain, Subnet, Bitcoin Address, E-mail address, Phone Number, Human Name, Username, and Network ASN. Below the input fields are three tabs: 'By Use Case', 'By Required Data', and 'By Module'. The 'By Use Case' tab is selected, showing two options: 'All' (selected) and 'Footprint'. The 'All' option is described as 'Get anything and everything about the target.' and notes that all SpiderFoot modules will be enabled. The 'Footprint' option is described as 'Understand what information this target exposes to the Internet.' and notes that it gains understanding through network perimeter, identities, and search engine use. Underneath these tabs are two more sections: 'Investigate' (described as 'Best for when you suspect the target to be malicious but need more information.') and 'Passive' (described as 'When you don't want the target to even suspect they are being investigated.'). Both of these sections note that as much information will be gathered without touching the target. At the bottom of the form is a red 'Run Scan Now' button.

Step 2: Define Target

Enter your target in one of these formats:

- **Domain:**
- **IP Address:**
- **Email Address:**
- **Person Name:**
- **Phone Number:**
- **Username:**

Step 3: Select Scan Type

Choose from predefined scan profiles:

- **All:** Uses all available modules (comprehensive but slow)
- **Footprint:** Basic footprint discovery
- **Investigate:** Deep investigation with correlation
- **Passive:** Only passive reconnaissance (no direct contact)

spiderfoot

New Scan Scans Settings

New Scan

Scan Name: project-Metasploit

Scan Target: 10.0.2.3

Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:

Domain Name: e.g. example.com
IPv4 Address: e.g. 1.2.3.4
IPv6 Address: e.g. 2606:4700:4700::1111
Hostname/Sub-domain: e.g. abc.example.com
Subnet: e.g. 1.2.3.0/24
Bitcoin Address: e.g. 1HesYJSP1QqyPEjnQqvzBL1wujrUNGe7R

E-mail address: e.g. bob@example.com
Phone Number: e.g. +12345678901 (E.164 format)
Human Name: e.g. "John Smith" (must be in quotes)
Username: e.g. "jsmith2000" (must be in quotes)
Network ASN: e.g. 1234

By Use Case By Required Data By Module

All Get anything and everything about the target.
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.

Footprint Understand what information this target exposes to the Internet.
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.

Investigate Best for when you suspect the target to be malicious but need more information.
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.

Passive When you don't want the target to even suspect they are being investigated.
As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.

Run Scan Now

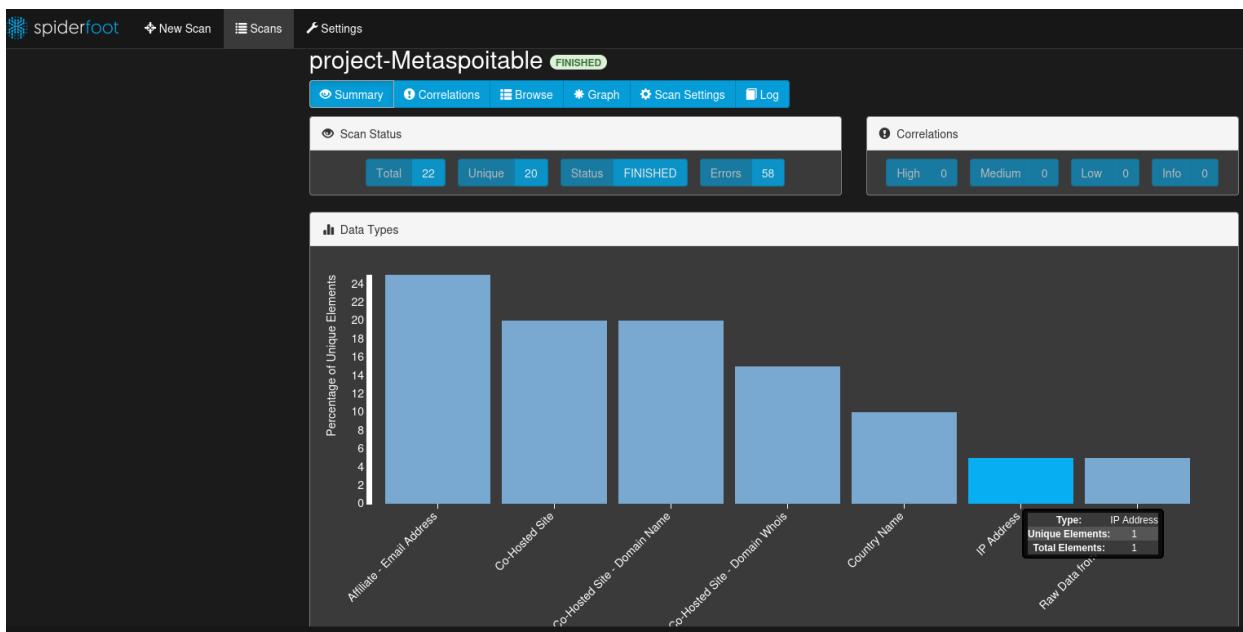
Step 4: Customize Modules (Optional)

Click **Show Advanced Options** to:

- Select specific modules
- Adjust timeout settings
- Configure thread count

Step 5: Start Scan

Click **Run Scan** button



Type	Unique Data Elements	Total Data Elements	Last Data Element
Affiliate - Email Address	5	5	2026-01-14 13:51:59
Co-Hosted Site	4	4	2026-01-14 13:51:33
Co-Hosted Site - Domain Name	4	4	2026-01-14 13:51:56
Co-Hosted Site - Domain Whois	3	3	2026-01-14 13:51:58
Country Name	2	4	2026-01-14 13:51:57
IP Address	1	1	2026-01-14 13:51:25
Open TCP Port	13	13	2026-01-14 13:53:13
Open TCP Port Banner	7	7	2026-01-14 13:52:42
Raw Data from RIRs/APIs	1	1	2026-01-14 13:51:32

Time	Component	Type	Event
2026-01-14 13:53:12	sfp_portscan_tcp	STATUS	TCP port 10.0.2.3:513 found to be OPEN.
2026-01-14 13:53:12	sfp_portscan_tcp	STATUS	TCP port 10.0.2.3:111 found to be OPEN.
2026-01-14 13:52:42	sfp_email	DEBUG	Received event, TCP_PORT_OPEN_BANNER, from sfp_portscan_tcp
2026-01-14 13:52:42	sfp_dnssresolve	DEBUG	Received event, TCP_PORT_OPEN_BANNER, from sfp_portscan_tcp
2026-01-14 13:52:42	sfp_stor_db	DEBUG	Storing an event: TCP_PORT_OPEN_BANNER
2026-01-14 13:52:42	sfp_stor_db	DEBUG	Storing an event: TCP_PORT_OPEN
2026-01-14 13:52:42	sfp_stor_db	DEBUG	Storing an event: TCP_PORT_OPEN

The screenshot shows a network scanning interface with the following details:

- Project Name:** project-Metaspoitable-2
- Status:** FINISHED
- Summary:** Summary tab is selected.
- Correlations:** Correlations tab is present.
- Browse:** Browse tab is present.
- Graph:** Graph tab is present.
- Scan Settings:** Scan Settings tab is present.
- Log:** Log tab is present.

Correlation Table:

Correlation	Risk	Data Elements
Database server exposed to the Internet: 10.0.2.3:3306	HIGH	1
Remote desktop exposed to the Internet: 10.0.2.3	HIGH	1
Software version revealed on open port: 220 (vsFTPD 2.3.4)	INFO	1
Software version revealed on open port: >	INFO	1
Software version revealed on open port: RFB 003.003	INFO	1
Software version revealed on open port: SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1	INFO	1

Monitoring Scan Progress

Real-time Monitoring

1. Navigate to **Scans** tab
2. Click on your active scan
3. View real-time results as they populate

Understanding the Results

Results are categorized into:

- **Entities:** Discovered assets (domains, IPs, emails, etc.)
- **Data Types:** Classification of findings
- **Modules:** Which module found the data
- **Correlation:** Relationships between entities



Analyzing Results

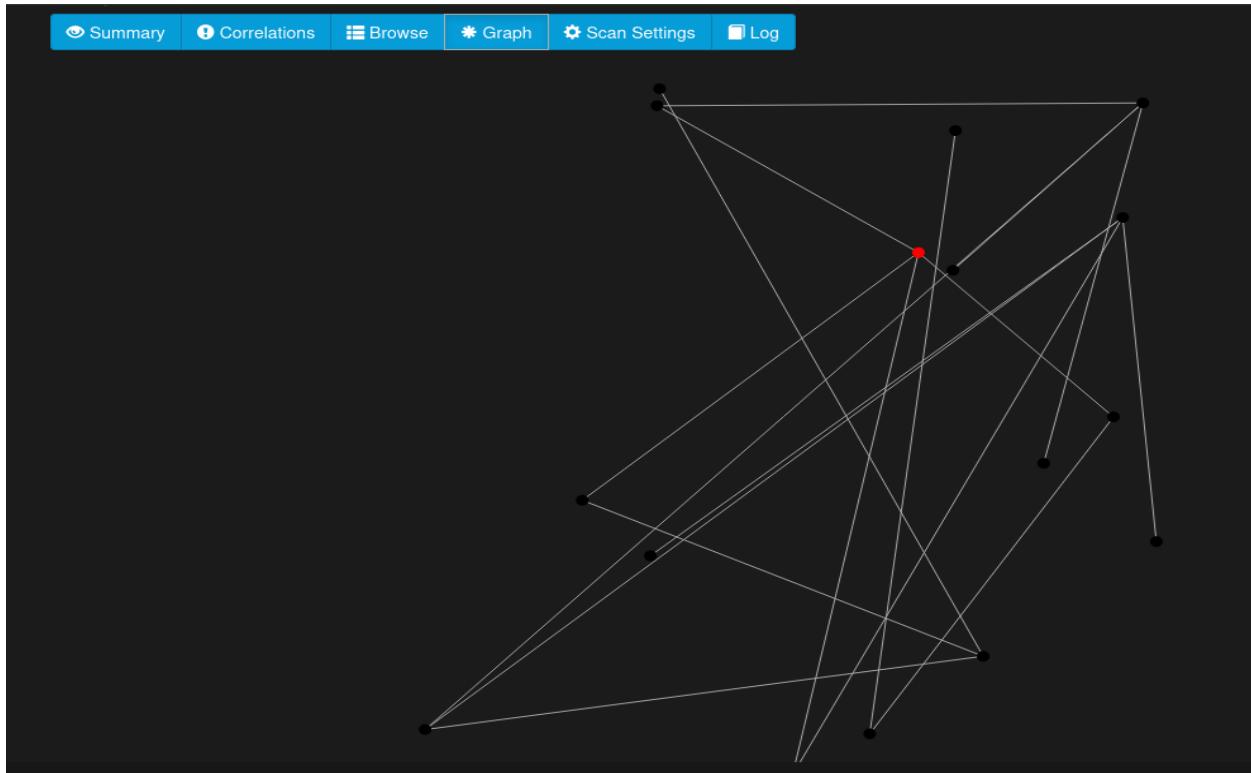
Step 1: Browse by Data Type

Click on different data categories:

- IP Addresses
- Domain Names
- Email Addresses
- Phone Numbers
- Physical Addresses
- Social Media Profiles
- Vulnerabilities

Step 2: View Relationships

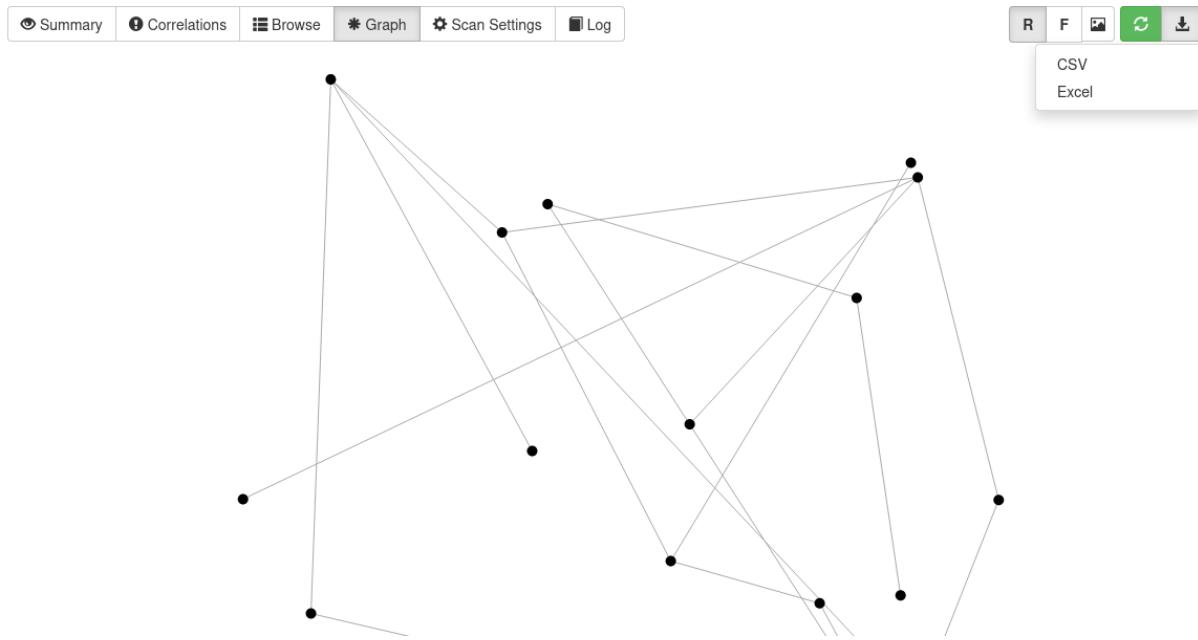
Click on **Graph** tab to see visual representation of relationships between discovered entities.



Step 3: Export Results

1. Click **Export** button
2. Choose format (JSON, CSV, GEXF)
3. Download file

project-Metaspoitable-2 FINISHED



← → ⌂ http://127.0.0.1:5000/scaninfo?d=C77F9C7C

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB SOC Radar LABS - Test... MITRE ATT&CK & ATT&CK

spiderfoot New Scan Scans Settings

project-Metaspoitable-2 FINISHED

Summary Correlations Browse Graph Scan Settings Log

CSV Excel

SpiderFoot-C77F9C7C.log.csv Completed — 143 KB

Show all downloads

Time	Component	Type	Event
2026-01-14 13:53:12	sfp_portscan_tcp	STATUS	TCP port 10.0.2.3:513 found to be OPEN.

Useful Command Options

Option	Description	Example
-s	Target to scan	-s example.com
-m	Modules to use	-m sfp_dnsresolve,sfp_whois
-o	Output format	-o json
-l	Listen address:port	-l 127.0.0.1:5001
-q	Quiet mode	-q
-t	Scan type	-t footprint

Practical Use Cases

Use Case 1: Company Security Assessment

Objective: Assess your organization's digital footprint

Steps:

1. Start a new scan with company domain
2. Select "All" scan type
3. Review discovered assets:
 - o Subdomains
 - o IP addresses
 - o Email addresses
 - o Exposed services
 - o Security vulnerabilities

4. Identify shadow IT and unknown assets
5. Document findings for remediation.

Use Case 2: Threat Intelligence Gathering

Objective: Collect intelligence on potential threats

Steps:

1. Enter suspicious domain or IP
2. Enable threat intelligence modules
3. Check for:
 - o Malware associations
 - o Blacklist status
 - o Historical DNS records
 - o Related infrastructure
4. Export findings for threat analysis

Use Case 3: Pre-Engagement Reconnaissance

Objective: Gather information before penetration testing

Steps:

1. Create passive-only scan
2. Collect publicly available information
3. Map attack surface
4. Identify potential entry points
5. Document for penetration test planning

Use Case 4: Brand Monitoring

Objective: Monitor brand mentions and exposure

Steps:

1. Scan company name as target
2. Enable social media modules
3. Track:
 - o Social media profiles
 - o Mentions across platforms
 - o Potential typosquatting domains
 - o Unauthorized brand usage

Use Case 5: Data Breach Investigation

Objective: Determine if company data was exposed

Steps:

1. Enter company domain and email patterns
2. Enable breach data modules (HaveIBeenPwned, etc.)
3. Review compromised credentials
4. Cross-reference with employee database
5. Initiate password reset procedures.

Advantages and Disadvantages

Advantages

1. Comprehensive Data Collection

- Integrates 200+ data sources in one tool
- Eliminates need for multiple separate tools
- Provides holistic view of target

2. Automation and Efficiency

- Automates tedious manual OSINT tasks
- Saves hours or days of research time
- Runs multiple queries simultaneously

3. User-Friendly Interface

- Intuitive web-based GUI
- Visual data correlation and graphing
- Easy navigation for beginners

4. Customization and Flexibility

- Modular architecture allows selective scanning
- Customizable scan profiles
- CLI support for automation

5. Active Development and Community

- Regularly updated with new modules
- Active community support
- Open-source and free to use

6. Data Correlation Intelligence

- Automatically links related information
- Discovers hidden relationships
- Provides context to findings

7. Export and Reporting

- Multiple export formats
- Integration-ready outputs
- Shareable reports

8. No Direct Target Contact (Passive Mode)

- Can operate entirely passively
- Reduces detection risk
- Ethical reconnaissance option

Disadvantages

1. API Key Dependencies

- Many advanced features require API keys
- Some services have usage limits
- Cost associated with premium API access

2. Rate Limiting Issues

- Free API tiers have restrictions
- May require time between scans
- Can slow down comprehensive scans

3. Resource Intensive

- Full scans can take hours
- High memory usage with multiple modules
- Network bandwidth consumption

4. Learning Curve

- Understanding module purposes takes time
- Interpreting results requires OSINT knowledge
- Advanced configuration can be complex

5. False Positives

- Not all discovered data is relevant
- Requires manual verification
- Can generate information overload

6. Data Accuracy Concerns

- Relies on third-party data sources
- Information may be outdated
- No guarantee of data correctness

7. Legal and Ethical Risks

- Improper use can violate laws
- Requires understanding of legal boundaries
- Easy to accidentally cross ethical lines

8. Privacy Implications

- Can reveal sensitive information
- Potential for misuse
- Ethical considerations required

Best Practices

Security Best Practices

1. Use in Controlled Environment

- Run on dedicated security testing systems
- Isolate from production networks
- Use VPN for additional privacy

2. Secure Your Installation

- Use strong passwords for web interface
- Restrict network access (use 127.0.0.1)
- Keep SpiderFoot updated regularly

3. Protect API Keys

- Store keys securely
- Never commit keys to version control
- Rotate keys periodically

Operational Best Practices

1. Start with Passive Scans

- Begin with passive reconnaissance
- Minimize target interaction
- Reduce detection footprint

2. Use Targeted Modules

- Don't always run "All" scans
- Select relevant modules for your objective
- Improves speed and reduces noise

3. Document Your Findings

- Export results regularly
- Maintain scan history

- Create reports for stakeholders

4. Verify Critical Findings

- Manually verify important discoveries
- Cross-reference with multiple sources
- Don't rely solely on automated results

5. Respect Rate Limits

- Space out comprehensive scans
- Monitor API quota usage
- Avoid overwhelming data sources

Ethical Best Practices

1. Obtain Proper Authorization

- Only scan assets you own or have permission to test
- Document authorization in writing
- Respect scope boundaries

2. Protect Discovered Data

- Handle sensitive findings responsibly
- Encrypt exported data
- Follow data protection regulations

3. Be Transparent

- Disclose your activities to appropriate parties
- Report vulnerabilities responsibly
- Avoid deceptive practices

Legal and Ethical Considerations

Legal Framework

What is Legal

Permitted Activities:

- Scanning your own assets and infrastructure
- Testing with written authorization
- Collecting publicly available information
- Security research on owned systems
- Educational purposes on test environments

What is Illegal

Prohibited Activities:

- Unauthorized access to systems
- Scanning without permission
- Using discovered credentials without authorization
- Violating computer fraud and abuse laws
- Circumventing security controls

Key Legal Regulations

United States

- **Computer Fraud and Abuse Act (CFAA)**: Prohibits unauthorized access
- **Electronic Communications Privacy Act (ECPA)**: Protects electronic communications
- **State Laws**: Many states have additional cybersecurity laws

European Union

- **GDPR**: Governs personal data processing
- **Network and Information Security (NIS) Directive**: Security requirements
- **National Cybercrime Laws**: Vary by member state

International

- **Council of Europe Cybercrime Convention:** International framework
- **Local Laws:** Always research target country's regulations

Ethical Guidelines

Professional Ethics

1. **Informed Consent:** Always obtain explicit permission
2. **Scope Limitation:** Stay within authorized boundaries
3. **Data Protection:** Safeguard discovered information
4. **Responsible Disclosure:** Report vulnerabilities appropriately
5. **Transparency:** Be honest about your activities

Risk Assessment Questions

Before conducting any scan, ask yourself:

- Do I have explicit written permission?
- Am I authorized to access this information?
- Could this activity cause harm or disruption?
- Am I following organizational policies?
- Have I documented my authorization?

Responsible Disclosure

If you discover vulnerabilities:

1. **Document the Finding**
 - Record detailed information
 - Take screenshots as evidence
 - Note date and time
2. **Notify Affected Party**

- Contact the security team or the responsible person
- Provide clear, technical details
- Give reasonable time to remediate

3. Don't Exploit

- Never use vulnerabilities for personal gain
- Don't access data beyond what's necessary to confirm
- Respect for embargo periods

4. Follow Disclosure Policies

- Check if the organization has a bug bounty program
- Follow coordinated disclosure timelines
- Use encrypted communication

Conclusion

SpiderFoot is a powerful OSINT automation tool that significantly enhances the efficiency and comprehensiveness of intelligence gathering operations. When used responsibly and ethically, it provides invaluable insights for security assessments, threat intelligence, and reconnaissance activities.

Key Takeaways

- SpiderFoot automates OSINT collection from 200+ sources
- Offers both web GUI and CLI interfaces for flexibility
- Requires proper authorization and ethical use
- Provides comprehensive data correlation and visualization
- Active open-source community and regular updates